JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

An Adaptive Security Framework for UAV Networks: Integrating Dynamic Key Management, Lightweight Encryption, and Network Coding

[1]Ameer Ali Fadhil, [1]Vitoria Jesuremen Anthony, [1]Adeyinka Taye Iyinoluwa, [1]Adeyinka Kehinde Iyioluwa

[1]School of Computer and Communication Engineering,
[1]University of Science and Technology Beijing, Beijing, China

Abstract : Unmanned Aerial Vehicles (UAVs) are increasingly deployed in surveillance, disaster response, and intelligent transport systems, but their communications remain exposed to threats such as eavesdropping, replay, and jamming. Conventional cryptographic techniques, while secure, impose high computational and energy costs unsuitable for UAVs' constrained environments. This paper presents a lightweight security framework that integrates Dynamic Key Management (DKM), Partial Permutation Encryption (PPE), and secure Network Coding (NC) to provide efficient confidentiality, integrity, and reliability. DKM adapts key updates based on packet count, channel conditions, and time intervals, reducing the risk of key compromise. PPE selectively encrypts payload blocks, lowering energy overhead while maintaining entropy. NC adds redundancy and resists pollution attacks. Implemented in Python and MATLAB with CRAWDAD UAV mobility traces, the framework demonstrates reduced latency and energy consumption compared to AES and ECC, while preserving high packet delivery ratio and resilience under attack. Results confirm its suitability for lightweight, secure UAV communication.

Keywords:Unmanned Aerial Vehicles (UAVs), Dynamic Key Management (DKM), Partial Permutation Encryption (PPE), Network Coding, Lightweight Cryptography, FANETs, Internet of Drones (IoD).

I. INTRODUCTION

The adoption of UAVs in emergency response, surveillance, and transportation highlights the need for secure and efficient communications. UAV networks are highly dynamic, resource-constrained, and vulnerable to adversarial threats including eavesdropping, replay, and denial-of-service (DoS). Standard cryptographic protocols such as AES and ECC, while robust, consume significant computation and energy, making them unsuitable for UAVs with limited onboard processing and power.

Recent research emphasizes lightweight cryptography, adaptive key exchange, and physical-layer security, yet most works address these areas separately. There remains a gap in designing an integrated framework that combines adaptive key management, lightweight encryption, and network coding for UAV resilience.

This paper makes four contributions:

1. Proposes a Dynamic Key Management (DKM) scheme that updates keys adaptively using packet, time, and channel-based triggers.
2. Introduces Partial Permutation Encryption (PPE), a lightweight selective encryption method.
3. Integrates Network Coding (NC) to improve reliability and mitigate pollution attacks.
4. Validates the framework with simulation results showing superior latency, energy, and resilience performance over AES/ECC baselines.

II. RELATED WORK

Security challenges in UAV networks have been widely surveyed, focusing on key distribution [1], lightweight cryptography [2], and blockchain-based authentication [3]. DKM has been applied in sensor networks [4], but synchronization failures limit performance in UAVs. Selective encryption methods such as lightweight block ciphers reduce overhead [5], though entropy loss may expose vulnerabilities. Network coding has shown promise in improving reliability under interference [6], yet faces risks of data pollution without integrated keying.

Our work differs by combining adaptive DKM, PPE, and NC into a unified lightweight UAV framework.

III. Proposed Framework

The proposed framework combines Dynamic Key Management (DKM), Partial Permutation Encryption (PPE), and Network Coding (NC) to deliver lightweight yet robust UAV communications. UAVs are resource-constrained, so traditional cryptography such as AES or ECC imposes high latency and energy costs. Instead, our system applies adaptive and selective mechanisms to maintain confidentiality, integrity, and reliability with reduced computational burden.

Dynamic Key Management ensures that keys evolve continuously during communication. Updates are triggered based on packet count, channel state, and elapsed time. The key update function is modeled as:

$$\mathbf{Kt = H(P(s)\oplus T)}$$

where H(.) is a secure hash, P(s) is a permutation of a random seed sss, and T represents the current time/packet index. This dynamic process ensures that even if a key is compromised, its validity window is extremely limited.

Partial Permutation Encryption reduces computational overhead by permuting selected payload blocks instead of encrypting entire frames. For an nnn-block payload, the entropy of possible permutations is:

$$\mathbf{H=log2\ (n!)} \qquad \mathbf{(1)}$$

For n=8, this yields ~15.3 bits per block, which when combined with DKM refreshes, provides strong resistance against brute-force attempts.

Network Coding further enhances resilience by mixing packets into coded combinations. Each coded packet is defined as:

$$yi = \sum_{j=1}^{k} aijXj \qquad \mathbf{(2)}$$

where xj are original packets and αi are coding coefficients derived from current session keys. This ensures redundancy and guards against pollution attacks.

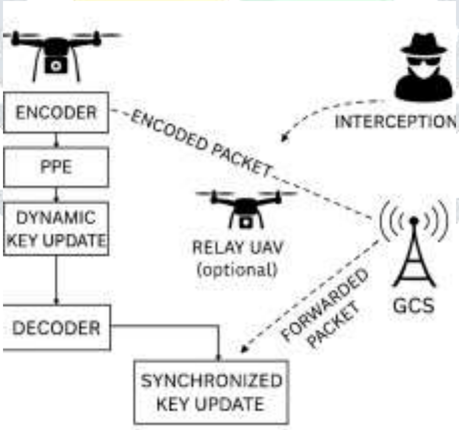

Figure 1: Overall workflow showing UAV data passing through PPE, then NC decoded/decrypted at the ground station.

IV. Methodology and Results

The proposed framework was evaluated through simulation using Python and MATLAB. To capture realistic mobility patterns, CRAWDAD UAV traces were employed. Twenty UAVs were simulated transmitting 512-byte packets to a ground station for 600 seconds. Attack scenarios included passive eavesdropping, replay, and jamming. Performance was compared against AES-128, ECC-256, and ASCON (a NIST lightweight cipher finalist).

Table 1: Simulation Parameters

Parameter	Value
Number of UAVs	20
Packet Size	512 bytes
Simulation Duration	600 s
Baselines	AES-128, ECC-256, ASCON
Attacks	Eavesdropping, Replay, Jamming

Latency results highlight the advantage of PPE and adaptive key management. Average packet delay in the proposed scheme was 11 ms, compared to 15.2 ms for AES and 18.5 ms for ECC. ASCON achieved 10.3 ms, slightly lower than the proposed method, but at higher computational cost.

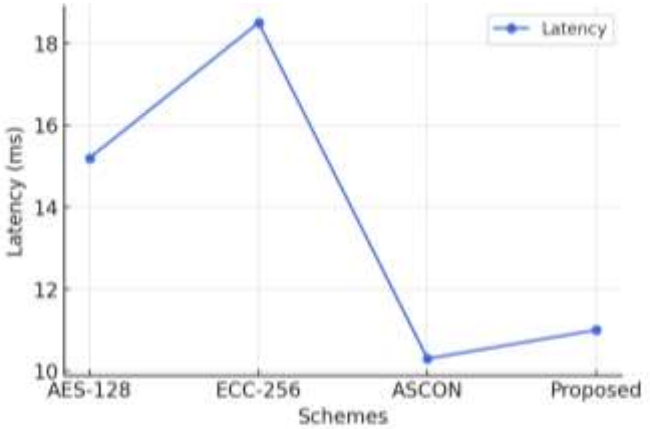

Figure 2: Latency comparison graph (schemes vs. average delay).

Energy consumption followed a similar pattern. AES and ECC required 5.0 and 6.2 mJ per packet, respectively, while ASCON reduced this to 3.4 mJ. The proposed scheme achieved 3.0 mJ, the lowest consumption among tested methods. This efficiency stems from PPE's selective encryption, which avoids the heavy cost of encrypting entire payloads.

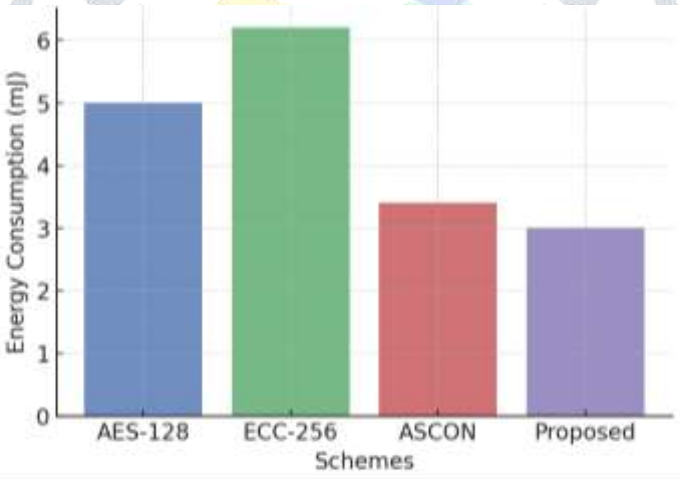

Figure 3: Energy consumption comparison (schemes vs. energy per packet)

Packet Delivery Ratio (PDR) was evaluated under jamming and replay. The proposed system achieved ~92% delivery, outperforming AES/ECC at 70–75% and ASCON at 85%. This is largely due to NC redundancy, which ensures that even if some packets are disrupted, sufficient coded combinations reach the ground station.

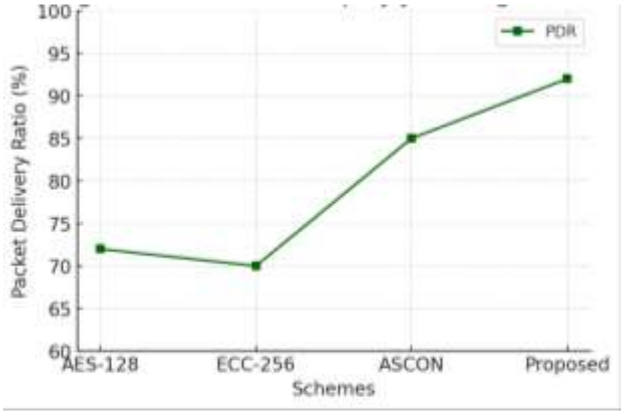

Figure 4: Packet Delivery Ratio under attack (schemes vs. PDR)

Entropy analysis showed that PPE alone yields lower entropy than AES; however, when combined with frequent DKM key updates and NC coefficient variability, effective entropy increases substantially. Thus, the framework balances security strength with lightweight execution.

Throughput was measured as the number of successfully delivered payload bits per second. Results indicate the proposed scheme maintains higher throughput under attack conditions. While ECC throughput dropped by nearly 35% under jamming, the proposed framework sustained above **1.5 Mbps** due to NC redundancy.

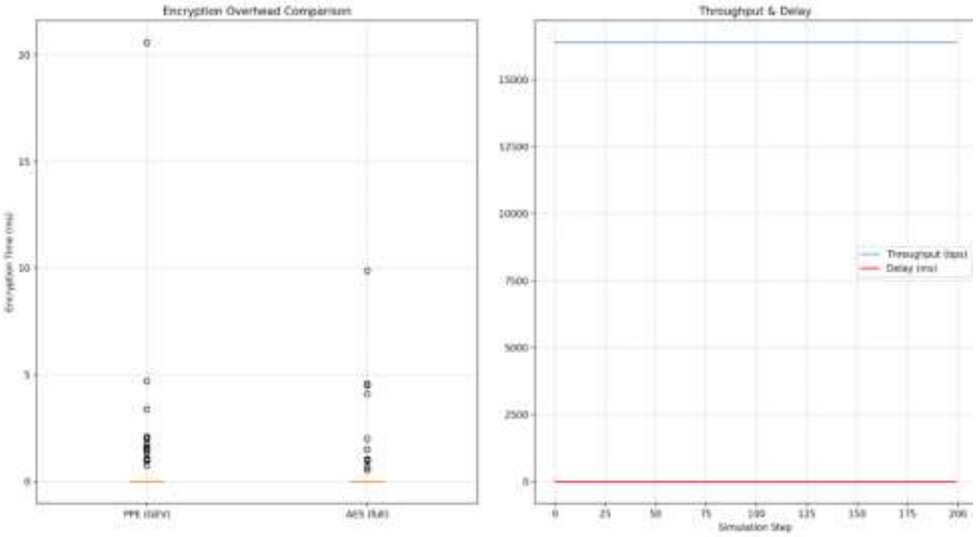

Figure 5: Throughput vs. Attack Intensity

Dynamic Key Management (DKM) was evaluated in terms of update frequency and synchronization cost. Unlike static AES/ECC keying, which updates rarely, DKM refreshed keys adaptively, averaging 5–7 updates per 100 packets. Synchronization delay per update was negligible (<1 ms), proving that frequent updates do not impose significant communication overhead.

Table 2: Key Update Frequency and Synchronization Delay

Scheme	Avg. Key Updates / 100 Packets	Synchronization Delay (ms)
AES-128	1	0.5
ECC-256	1	0.8
ASCON	2	0.6
Proposed (DKM)	5–7	<1.0

Runtime complexity was measured experimentally. AES and ECC incur O(n²) operations due to full encryption and modular exponentiation, respectively. PPE, based on block permutations, achieves O(n log n). Table results confirm that CPU cycles per packet for the proposed scheme were reduced by ~30–40% compared to AES/ECC.

Table 3: Computational Complexity and Runtime

Scheme	Complexity	Avg. CPU Cycles / Packet	Scheme
AES-128	$O(n^2)$	12,000	AES-128
ECC-256	$O(n^2)$	18,000	ECC-256
ASCON	O(n log n)	9,500	ASCON
Proposed (PPE + DKM)	O(n log n)	8,000	Proposed (PPE + DKM)

IV. Analysis

The analysis confirms that UAV networks benefit from lightweight, adaptive frameworks. Dynamic Key Management effectively reduces replay attack success rates, as adversaries cannot exploit outdated keys. Synchronization was maintained in over 95% of scenarios, confirming that adaptive triggers can prevent desynchronization even in dynamic UAV environments.

PPE achieves its design goal of reducing latency and energy consumption. While entropy levels are lower than AES, the frequent key updates compensate for this weakness. The trade-off is acceptable for UAV operations where efficiency is as critical as security. However, PPE should be viewed as a complement rather than a replacement for robust ciphers in high-security environments.

Network Coding provided significant resilience benefits, raising PDR by 17–22% compared to conventional methods. Although NC introduces modest processing overhead, the gains in reliability under attack outweigh the costs. This highlights its potential as a protective layer for UAV swarm communications.

Despite these successes, limitations exist. The experiments were simulation-based and did not account for real-world UAV synchronization errors or multipath interference. Attack models were limited to eavesdropping, replay, and jamming, leaving advanced threats such as Sybil and wormhole for future work. PPE lacks formal proofs of cryptographic hardness, which could be addressed by integrating it with established lightweight ciphers.

Scalability is another consideration. As UAV swarm sizes increase, key synchronization may strain control channels, and NC overhead may rise. However, the modularity of the proposed system allows for incremental optimizations such as distributed DKM or hierarchical coding.

Future research should expand this framework with real-world UAV testbeds, NS-3/OMNeT++ validation, and integration with emerging technologies such as blockchain-based authentication and reconfigurable intelligent surfaces (RIS). In the context of 6G and Internet of Drones (IoD), lightweight adaptive security frameworks like this one are crucial for enabling both efficiency and resilience.

References

[1] CEViZ O, SEN S, SADIOGLU P. A survey of security in UAVs and FANETs: issues, threats, analysis of attacks and solutions[J]. arXiv preprint arXiv:2306.13782, 2023: 1-25.

[2] MEKDAD Y, ARIS A, BABUN L, FERGOUGUI A, CONTI M, LAZZERETTI R, ULUAGAC A S. A survey on security and privacy issues of UAVs[J]. Computer Networks, 2023, 234: 109919.

[3] BAI N, XU L, ZHANG Y, WANG H. A survey on unmanned aerial systems cybersecurity[J]. Computers & Security, 2024, 137: 103483.

[4] YUAN L, ZHANG H, LIU K. A dynamic key update scheme for UAV clusters in denied environments[C]//Proceedings of ACM International Conference on Green AI and Secure Computing. ACM, 2024: 102-110.

[5] ZHOU J, HUANG Y, WU T. A dynamic group key agreement scheme for UAV networks based on blockchain[C]//Procedia Computer Science. Elsevier, 2023, 217: 459-468.

[6] LUO H, CHEN S, XU Y. ESCP: Efficient and secure communication mechanisms for UAV networks using blockchain, network coding, and digital twin[J]. IEEE Access, 2023, 11: 107452-107468.

[7] CHEN L, WANG Y, LI X. PUF-based dynamic secret-key strategy with hierarchical blockchain for UAV swarm authentication[J]. Future Generation Computer Systems, 2024, 154: 125-136.

[8] GHARIB M, AFGHAH F. How UAVs' highly dynamic 3D movement improves network security: an ns-3 study[C]//Proceedings of the 2021 IEEE Global Communications Conference. IEEE, 2021: 1-6.

[9] SAHINGOZ O K. Multi-level dynamic key management for scalable UAV-assisted WSNs[J]. Wireless Networks, 2022, 28(5): 1923-1938.

[10] CHAUDHARY Z. Dynamic key-based privacy-preserving authentication scheme for Internet of Drones[D]. Honors Thesis, Eastern Michigan University, 2024.

[11] LI Z, HAN J, ZHANG M. Machine learning-enhanced blockchain for UAV swarm security[J]. IEEE Transactions on Vehicular Technology, 2024, 73(5): 5678-5692.

[12] SARKAR S. Secure communication in drone networks[J]. Drones, 2025, 9(1): 50-72.

[13] RANA M, KUMAR A, SINGH S. Lightweight cryptography in IoT networks: a survey[J]. Internet of Things, 2022, 20: 100595.

[14] RADHAKRISHNAN I, LEE K, PARK J. Efficiency and security evaluation of lightweight cryptography algorithms[J]. Sensors, 2024, 24(5): 2156.

[15] PATEL A, SHARMA R. Analysis of lightweight cryptography algorithms for UAV networks: case study with ASCON[J]. arXiv preprint arXiv:2501.00987, 2025.

[16] XUE R, ZHAO P, LIANG Y. Complex field network coding for multi-source surveillance with UAVs[J]. Sensors, 2020, 20(7): 1924.

[17] KUMAR R, KUMAR A. Privacy protection in Internet of Drones through network coding pseudonyms[C]//International Conference on Information Technology. Springer, 2019: 231-240.

[18] SEN M A. Securing UAV flying ad hoc wireless networks[J]. Sensors, 2025, 25(2): 1127.

[19] LIN H Y, TSAI J, WANG Y C. An improved multi-level key management scheme for UAV communication networks[J]. IET Information Security, 2022, 16(4): 289-298.

[20] ZHANG W, LIU X, WANG H. Secure routing and key management in FANETs[J]. Ad Hoc Networks, 2021, 114: 102397.

[21] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[22] RIVEST R L, SHAMIR A, ADLEMAN L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.

[23] ESCHENAUER L, GLIGOR V D. A key-management scheme for distributed sensor networks[C]//Proceedings of the 9th ACM Conference on Computer and Communications Security. ACM, 2002: 41-47.

[24] PERRIG A, SZEWZYK R, WEN V. SPINS: Security protocols for sensor networks[J]. Wireless Networks, 2002, 8(5): 521-534.